# AUTHENTICATING METHOD IN COMMUNICATION SYSTEM, CENTER EQUIPMENT, AND RECORDING MEDIUM WITH AUTHENTICATION PROGRAM RECORDED THEREON

**Publication number:** JP2001177513
**Publication date:** 2001-06-29
**Inventor:** SHIMAMURA YUICHI; MAIDA IZUMI; AOKI TAKAHIRO
**Applicant:** NIPPON TELEGRAPH & TELEPHONE
**Classification:**
**- international:** ***H04L9/08; G06F15/00; G06F21/20; H04L9/32;*** **H04L9/08; G06F15/00; G06F21/20; H04L9/32;** (IPC1-7): H04L9/08
**- European:**
**Application number:** JP19990356105 19991215
**Priority number(s):** JP19990356105 19991215



Abstract of **JP2001177513**

PROBLEM TO BE SOLVED: To change cryptographic keys used for encryption each time an authentication token is prepared even without performing communication between two pieces of center equipment whenever a communication terminal authenticated by one center equipment communicates with the other center equipment. SOLUTION: When center equipment 3 authenticates the communication terminal 1, the equipment 3 generates a session key (b) from a master key 332 periodically shared between center equipment 4 and the equipment 3 and a random value (a), acquires a center identifier 321 and a user ID 341, generates an authentication token (c), generates an authentication code (d) obtained by connecting the random value (a), the authentication token (c) and a master key ID 331 and transmits the authentication code (d) to the terminal 1. The terminal 1 transmits the code (d) to the equipment 4 in the case of communicating with the equipment 4. The equipment 4 decomposes the code 4 to acquire a master key 432, generates a session key (b), decodes the token (c), verifies the propriety of the equipment 3 and specifies the user.